Сюзанна Борншлегл, *MEN Mikro Elektronik*

Промышленные компьютеры для приложений повышенной функциональной безопасности

В статье рассматриваются вопросы построения систем повышенной функциональной безопасности на основе одноплатных компьютеров. В последнее время спрос на такие системы растёт, и они требуются для различных областей нашей жизни. Встраиваемые промышленные компьютеры способны решать задачи любой сложности в достаточной тяжёлых условиях эксплуатации, но лишь немногие могут соответствовать требованиям по безопасности. Это связано прежде всего со сложной процедурой сертификации, что значительно повышает стоимость системы. Поэтому открыт вопрос, есть ли готовые COTS-решения для приложений повышенной функциональной безопасности?

В современной жизни нам всё чаще приходится доверять электронным системам управления, контролирующим работу общественного транспорта и средства передвижения. И мы должны быть уверены в их безопасной работе. Данные системы должны соответствовать многим специализированным стандартам, специфичным для конкретных областей, как например авиация и железная дорога. Наличие сертификатов, конечно, может гарантировать безопасность, но всё же остаётся главный вопрос – на каком оборудовании выполнены данные системы?

Как показывает практика, чаще всего применяются стандартные промышленные компоненты (COTS). Компания *MEN* поставила перед собой задачу разработать промышленные процессорные платы в двух стандартах – VME и CPCI, которые хорошо себя зарекомендовали в качестве основы для построения высоконадёжных систем управления. Эти платы требовалось выполнить с учётом повышенных требований по функциональной безопасности, с одновременным сохранением их возможности относится к разряду стандартных (COTS) коммерческих компонентов.

Само собой разумеется, что оба эти продукта не совсем обычны. И далее будет показано, благодаря чему они такие особенные. В них, естественно, закладываются все известные принципы построения высоконадёжных систем для приложений повышенной функциональной безопасности. Одним из таких решений является резервирование. Системный компонент, вызывающий в случаи неисправности остановку всей системы, является единой точкой отказа. В худшем случаи отказ такого компонента может привести к большому ущербу или вызвать опасность для человеческой жизни. Вот почему все критические компоненты всегда дублируются. Будучи идентичны, они могут сохранить систему в рабочем состоянии даже в случае выхода из строя одного из них. Например, системы управления самолётом должны всегда оставаться в работе, даже если вышел из строя один из компонентов. Отказоу-

стойчивые системы должны проектироваться так, чтобы в случае неисправности одного из узлов система в целом продолжала свою работу. В зависимости от различных сценариев существует несколько вариантов построения резервируемых систем – от «один-из-двух» (1oo2) до «два-из-четырёх» (2oo4). Специализированное устройство сравнивает выходные значения и определяет, как система должна реагировать.

Инженеры компании *MEN* хорошо знакомы с архитектурой резервирования. Они, например, разрабатывали системы «два-из-трёх» с тремя одинаковыми процессорными платами на базе стандарта CompactPCI. Такой тип резервирования очень распространён. Происходит мажоритарная выборка результатов, и набравший большинство вариантов результат является определяющим для управления системой. Применение COTS-компонентов для построения резервированных систем на основе открытых стандартов может казаться эффективным способом, но и у него есть свои недостатки: необходимы специализированное программное обеспечение и устройства ввода-вывода для синхронизации трёх систем и организации мажоритарной выборки. Это может снизить производительность всей системы при повышении энергопотребления (необходимо запитывать сразу три системы) и увеличении занимаемого системой пространства.

Процессорные платы компании MEN D602 и A602 уже идут с тройным резервированием «на борту». Это значит, что процессоры PowerPC 750, оперативная память, локальные источники питания, флэш-память и генераторы синхросигналов резервируются (рис. 1). Другой важный функционал, запрограммированный в ПЛИС, также имеет тройное резервирование. К этому функционалу относятся и регистры, производящие мажоритарную выборку. Таким образом, система в целом остаётся работоспособной даже при неисправности одного их компонентов.

Такое решение «всё-в-одном» имеет ряд преимуществ, таких как более низкое энергопотребление и занимаемое пространство, по сравнению с системами, построенными на стандартных компонентах. В качестве запрограммированной в ПЛИС логики для организации работы трёх процессоров PowerPC и других важных компонентов, выбрана архитектура lock-step (жёстко регламентированная архитектура). Это означает, что идентичные компоненты работают синхронно, всегда выполняют одну и ту же задачу и для выполняемого программного обеспечения они видятся как один элемент. Таким образом, может применяться программное обеспечение, разработанное для стандартной однопроцессорной системы, что

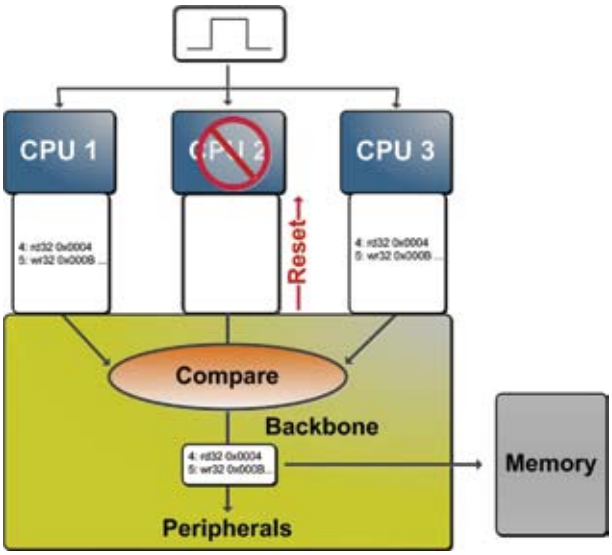

Рис. 1. Изоляция неисправности при тройном резервировании ЦПУ

значительно упрощает интеграцию ПО и снижает издержки и затраты на её разработку. Для синхронизации трёх процессоров в случае возникновения неисправностей достаточен простой код. Кроме того обновление существующего программного обеспечения, основанного на однопроцессорном подходе, требует меньше затрат.

Дизайн «два-из-трёх» также менее чувствителен к аппаратным неисправностям и переходным процессам. Типовыми проблемами для авиационных приложений являются однократные и многократные сбои (SEU и MEU). Эти случайные события могут быть вызваны изменением информации в одном бите (с 0 на 1 или наоборот) в результате действия космической радиации. Единичный процессор или модуль памяти очень восприимчивы к одиночным сбоям (SEU).

Система с тройным резервированием динамической памяти автоматически корректирует подобные сбои. Циклы чтения и записи всегда осуществляются во все модули памяти. Механизм очистки памяти считывает информацию из всех ячеек, после чего происходит мажоритарная выборка и правильное значение записывается во все три модуля памяти. Это происходит для каждого цикла обновления и предотвращает накопление ошибочных битов в течение долгого времени.

Чтобы получить отказоустойчивую и критичную по отношении к безопасности систему, необходимо иметь предсказуемое время выполнения операций. Это значит, что система должна реагировать на внешнее воздействие за определённое время, и это время должно быть неизменным при работе в самых жёстких условиях.

Процессорные платы D602/A602 созданы для строго детерминированной работы, и в них не применяются режимы прямого доступа к памяти (DMA) и прерывания, способные существенно повлиять на время реакции системы. Дополнительные механизмы диагностики позволяют выявлять скрытые ошибки прежде, чем они приведут к системным сбоям. Они включают в себя расширенные функции BITE (built-in test equipment), такие как счётчик количества ошибок в модулях памяти или мониторинг всех внутренних напряжений питания, что позволяет повысить функциональную безопасность работы системы и её работоспособность. Обе процессорные платы разработаны в соответствии со стандартами DO-254 (для авиации) и EN 50129 (для железных дорог). Плата D602 была разработана как компьютер с повышенной функциональной безопасностью для системы управления работой грузовым отсеком в самолёте Airbus A400M и сейчас доступна как стандартный COTS-компонент для систем CPCI.

Также процессорные платы D602/A602 разработаны в соответствии со стандартами DO-160 и EN 50155 (внешние воздействующие факторы). Они предназначены для работы в диапазоне температур от –40 до +50 °C, при высоте до 20000 метров. В исполнении с кондуктивным теплоотводом они способны работать до +70 °C. Учитывая эти данные, может быть получена сертификация по самым строгим уровням безопасности – SIL 4 в железнодорожных или DAL-A в авиационных приложениях.

Есть, однако, одно обстоятельство, которое может быть препятствием: данные стандарты требуют применения внутри системы разных аппаратных платформ. Причина в том, что идентичные резервируемые подсистемы очевидным образом являются источником мультиплицируемых параллельных отказов. Для преодоления подобных препятствий процессорные платы D602/A602 хорошо функционально оснащены, одним из путей обхода данной проблемы может быть использование разделения ресурсов PowerPC MMU (блок управления памятью). Несхожие, независимо разработанные программные приложения могут быть запущены в двух разделах, и могут использоваться различные аппаратные средства ввода-вывода. Эти различные аппаратно-программные способы позволяют сертифицировать платы по самым высоким уровням безопасности.

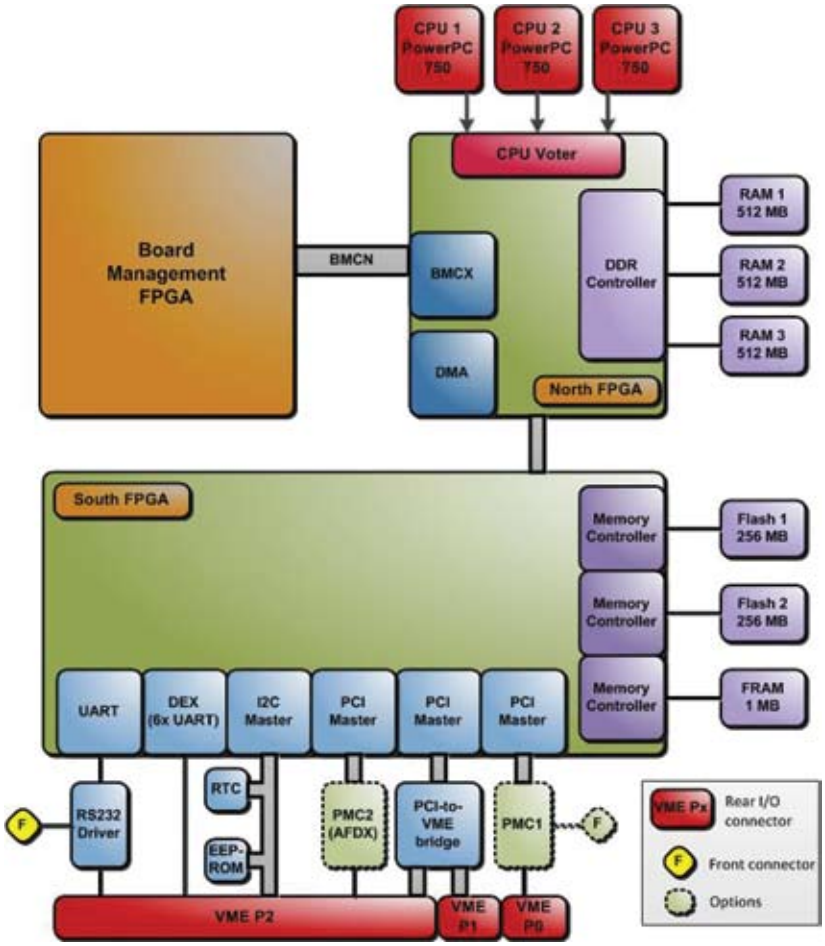

Рис. 2. Функциональная схема A602 – тройное резервирование «на борту»

Последним элементом сертификационной мозаики является операционная система (ОС). Процессорные платы D602 и A602 поддерживают целый ряд ОС, специально предназначенных для приложений повышенной функциональной безопасности, в частности различные ветви ОС VxWorks компании *Wind River* – от универсальной ОС реального времени (ОСРВ) VxWorks 6.x до специализированных ОС VxWorks Cert и VxWorks 653.

Специализированные ОС VxWorks Cert и VxWorks 653 поддерживают сертификацию по стандартам DO-178B/C и EUROCAE ED-12B (до уровня A включительно), а также IEC 61508 (до SIL 4 включительно); VxWorks 653 при этом поддерживает разделение ресурсов (resource partitioning), упомянутое выше, а также интеграцию приложений различных поставщиков согласно DO-297. Для обеих ОС – VxWorks Cert и VxWorks 653 – доступны готовые пакеты сертификационной доку-

Рис. 3. Процессорная плата A602

Рис. 4. Процессорная плата D602

ментации по всем поддерживаемым стандартам. Возможности быстрой загрузки, предоставляемые D602 и A602, обеспечивают время старта приложений в пределах 500 мс (при размере загрузочного образа 8 Мбайт), что позволяет приложениям стартовать практически мгновенно при включении устройства и быстро перезагружаться в случае сбоев по питанию.

Процессорная плата A602 выполнена в стандарте 64-bit VME и может использоваться в качестве мастера (рис. 2). А D602 – это системный процессор для систем CPCI. Обе выполнены в формфакторе Eurocard 6U. Они созданы на базе процессоров PowerPC 750 с рабочей частотой до 900 МГц. Оперативная память в объёме 512 Мбайт спроектирована по схеме тройного резервирования, в дополнение плата оснащена 256 Мбайт резервируемой флэш-памяти и одномегабайтным модулем FRAM. Для повышения надёжности работы применяются модули памяти и флэш с функцией коррекции ошибок (ECC). Стандартные функции ввода-вывода реализованы на ПЛИС и доступны через модуль тыльного ввода-вывода. К этим функциям относится: 6 последовательных портов, шина I²C, порт RS-232, который может быть доступен и на передней панели. Для реализации дополнительного функционала платы оснащены двумя разъёмами PMC, один из которых предназначен для организации протокола ADFX (ARINC 664) с тыльной стороны. Другой модуль PMC доступен на передней панели, но при исполнении с кондуктивным теплоотводом он может быть доступен также и с тыльной стороны.

Две процессорные платы, работающие совместно, могут стать основой для построения высоконадёжного кластера для задач с повышенными требованиями по функциональной безопасности. По сути, это два параллельно работающих канала, но доступен только один. При возникновении неисправности система автоматически переключается на другой. Для организации такой работы платы могут быть скоммутированы между собой по каналу BMCX, а с приложениями они будут работать с использованием шести последовательных портов. С учётом возможности работы этих плат в расширенном температурном диапазоне и годности к лётной эксплуатации, D602 (рис. 4) и A602 (рис. 3) могут использоваться в авиации для различных задач, таких как коммуникация, навигация, дисплей управления, управление полётом, погодные системы, системы предотвращения столкновений и т.д. А также могут быть использованы и для наземных систем управления, предъявляющих высокие требования по функциональной безопасности: связь, системы безопасности, радарные системы, системы управления трафиком. Кроме авиационного применения данные процессорные модули могут использоваться и на железнодорожном транспорте, как для управления работой поездов, так и в составе диспетчерских систем управления железнодорожным движением.

Кроме двух классических рынков, таких как авиация и железнодорожный транспорт, есть ещё много интересных направлений, где необходимы промышленные и в то же время обладающие повышенной функциональной безопасностью компьютеры. В целом это относится ко всем рынкам, где отказы могут привести к большим потерям. Это коммерция, логистика, производство, медицина и телекоммуникационная инфраструктура. Процессорные платы D602 и A602 компании *MEN Mikro Elektronik* могут стать надёжной базой построения систем для приложений повышенной функциональной безопасности.